AMENDMENTS TO THE CLAIMS

Upon entry of this amendment, the following listing of claims will replace all prior versions and listings of claims in the pending application.

IN THE CLAIMS

Please amend claims 1, 2, 3, 5, 7, 8, 9, 11, 13, 15, 17, 21, 22 and 26, and cancel claims 4, 10, 20 and 25, as follows:

1. (Currently Amended) A method of a device for filtering messages routed across a network, the messages including field name-value pairs, the method comprising:

extracting, by a filter configured on a device, field name-value pairs from messages received via a network;

determining, by a learning engine configured on the device, a most restrictive data type of values from a plurality of data types of values for a field name of the extracted field name-value pairs;

determining, by the learning engine, a match factor for a data type, the match factor indicating a fraction of values for the same field name that match the data type;

selecting, by the learning engine, a data type having a match factor exceeding a threshold and having no child data types with a match factor exceeding the threshold; and

storing, by the device, the most restrictive data type in association with the field name.

2. (Currently Amended) The method of claim 1, further comprising:

generating, by the learning engine ~~device~~, a rule which would allow messages having values of a field name that match the most restrictive data type.

3. (Currently Amended) The method of claim 2, further comprising:

applying, by the learning engine ~~device~~, the rule to determine whether to allow messages having values for a field name that match the most restrictive data type.

4. (Canceled).

5. (Currently Amended) The method of claim ~~4~~ 1, wherein the threshold is a fraction of values for the same field name which should match the data type.

6. (Canceled).

7. (Currently Amended) A method of a device for filtering Uniform Resource Locator (URL) messages routed across a network, wherein the messages include URL components, the method comprising:

extracting, by a filter configured on a device, URL components from messages received via a network;

determining, by a learning engine configured on the device, for URL components at a same level, with a same root URL component, a most restrictive data type from a plurality of data types of extracted URL components at the same level;

determining, by the learning engine , a match factor for a data type, the match factor indicating a fraction of URL components at the same level, with the same root URL component, that matches the data type; and

selecting, by the learning engine , a data type having a match factor exceeding a threshold and having no child data types with a match factor exceeding the threshold; and

storing, by the learning engine ~~device~~, the most restrictive data type in association with the URL components at the same level.

8. (Currently Amended) The method of claim 7, further comprising:

generating, by the learning engine ~~device~~, a rule which would allow messages having the URL components that match the most restrictive data type.

9. (Currently Amended) The method of claim 8, further comprising:

applying, by the learning engine ~~device~~, the rule to determine whether to allow messages having the URL components that match the most restrictive data type.

10. (Canceled).

11. (Currently Amended) The method of claim ~~10~~ 7, wherein the threshold is a fraction of URL components at the same level, with the same root URL component, which should match the data type.

12. (Canceled).

13. (Currently Amended) A method of a device for inferencing a data type of scalar objects from messages routed across a network, the method comprising:

identifying, by a message filter configured on a device, scalar objects from messages received via a network, each of the scalar objects having a data type from a plurality of data types;

determining, by learning engine configured on the device, a match factor for ~~a~~ each data type of the scalar objects, the match factor indicating a fraction of the scalar objects that match the data type; and

selecting, by the learning engine ~~device~~, a most restrictive data type from the plurality of data types of the scalar objects, the most restrictive data type having a match factor exceeding a threshold and having no child data types with a match factor exceeding the threshold.

14. (Original) The method of claim 13, wherein the threshold is a fraction of scalar objects which should match the data type.

15. (Currently Amended) A system for inferencing a data type of scalar objects from messages routed across a network, the system comprising:

a learning engine ~~module of~~ configured in a device for determining a match factor for ~~a~~ each data type of the scalar objects, the match factor indicating a fraction of scalar objects identified from messages received via a network that match the data type; and

wherein the learning engine ~~module of~~ the device selects a most restrictive data type from a plurality of data types of the scalar objects, the most restrictive data type having a match factor exceeding a threshold and having no child data types with a match factor exceeding the threshold.

16. (Canceled).

17. (Currently Amended) A system for filtering messages routed across a network, the messages including field name-value pairs, the system comprising:

a learning engine ~~of~~ configured on a device, for extracting field name-value pairs from messages received via a network, determining~~,~~ a most restrictive data type of values from a plurality of data types of values for a field name from the extracted field name-value pairs, and storing the most restrictive data type in association with the field name~~;~~, determining a match factor for a data type, the match factor indicating a fraction of values for the same field name that match the data type, and selecting a data type having a match factor exceeding a threshold and having no child data types with a match factor exceeding the threshold; and

a message filter ~~of~~ configured on the device~~,~~ for generating a rule which would allow messages having values of a field name that match the most restrictive data type.

18. (Original) The system of claim 17, wherein the learning engine is further adapted to generate a rule which would allow messages having values of a field name that match the most restrictive data type.

19. (Original) The system of claim 17, wherein the message filter is further adapted to apply the rule to determine whether to allow messages having values for a field name that match the most restrictive data type.

20. (Canceled).

21. (Currently Amended) The system of claim ~~20~~ 17, wherein the threshold is a fraction of values for the same field name which should match the data type.

22. (Currently Amended) A system for filtering Uniform Resource Locator (URL) messages routed across a network, wherein the messages include URL components, the system comprising:

a learning engine ~~of~~ configured on a device, for extracting URL components from messages received from a network, determining, for URL components at a same level, with ~~the~~ a same root URL component, a most restrictive data type from a plurality of data types of URL components at the same level, and storing the most restrictive data type in association with the URL components at the same level~~;~~, determining a match factor for a data type, the match factor indicating a fraction of URL components at the same level, with the same root URL component, that match the data type, and selecting a data type having a match factor exceeding a threshold and having no child data types with a match factor exceeding the threshold; and

a message filter ~~of~~ configured on the device, for generating a rule which would allow messages having the URL components that match the most restrictive data type.

23. (Original) The system of claim 22, wherein the learning engine is further adapted to generate a rule which would allow messages having the URL components that match the most restrictive data type.

24. (Original) The system of claim 22, wherein the message filter is further adapted to apply the rule to determine whether to allow messages having the URL components that match the most restrictive data type.

25. (Canceled).

26. (Currently Amended) The system of claim ~~25~~ 22, wherein the threshold is a fraction of URL components at the same level, with the same root URL component, which should match the data type.